The Shear et al. publication discloses cryptographic methods, apparatus and systems for storage media electronic rights management in closed and connected appliances, in which digital information 200, metadata 202 and associated controls 204 are stored on a storage medium 100, and that a key block 208 contains one or more cryptographic keys for decrypting the digital information 200 and the metadata 202. The key block 208 may itself be encrypted by hidden keys 210 stored in a location on the storage medium 100 not normally accessible.

The Downs et al. patent discloses an electronic content delivery system, in which an end-user device 109 includes player application 195 for scrambling the content 113 on receipt, and marks the content 113 with a copy/play code 523 representing the initial copy/play permission. The player application 195 generates a scrambling key for each of the received content 113, encrypts the scrambling keys and stores them in a hidden place in the end-user device 109. Then, each time the end-user device 109 accesses the content 113, the end-user device 109 verifies the copy/play code 523 before allowing descrambling of the content 113, and also updates the copy/play code of the content 113.

The Ginter et al. patent discloses systems and methods for secure transaction management and electronic rights protection, in which the one or more keys used to encrypt each permission record

808 or other management information record will be changed every time the record is updated.

Applicants submit that while Shear et al. discloses encrypting the digital work with an encryption key, and that the encryption key may be encrypted by a hidden key, Shear et al. neither discloses or suggests that the control should be encrypted by a hidden information.

With regard to Downs et al. Applicants submit that the digital work (content 113) is stored within the end-user device which can actively deny a user to access and modify the usage right, e.g., by storing such information deeply inside an integrated circuit. Applicants believe that Downs et al. is not relevant to the subject invention which claims a passive record carrier storing the information on a surface which is open for inspection.

Applicants submit that as with Downs et al., Ginter et al. stores the usage rights, i.e., the permission records with a device (see col. 136, lines 23-28). While Ginter et al. indicates, at col. 212, lines 43-52, that an encryption key should be periodically changed in order to lessen the time during which each key is used, giving an attacker less ciphertext to use in an attempt to obtain the key, Applicants urge that this is irrelevant to the subject invention. What matters, in the subject invention, is that the usage rights (a small quantity of ciphertext) are re-encrypted

after each change, where the encryption key is managed in such a way that it does not help an attacker to overwrite a newer version or the encrypted usage rights with an older version, in an attempt to undo consumption of one or more rights.

Applicants therefore believe that a record carrier, as claimed, is substantially different from an active device. Most notably, a typical passive record carrier is vulnerable against a "copy and restore" attack, which is explained in the Substitute Specification on page 5, line 20 to page 6, line 7 (paragraph [0012]), whereas an active device has no such vulnerability.

The Examiner now states that Shear et al. does disclose that the hidden information is used for encrypting or verifying the control information. "There are at least two ways in which this is done in Shear. The first stores control information and the key block within a secure container, and the hidden keys are used to encrypt and decrypt this container. The second stores the key block outside the secure container, uses the hidden keys to encrypt/decrypt the key block and uses keys from the key block to access the secure container, which contains the control information. This can be seen on Pages 9-10, in Paragraphs 129-142, as well as Pages 15-16, in paragraphs 216-220."

Applicants have reviewed these sections of Shear et al. and note that Shear et al. states "a secure 'software container' is provided that allows: Cryptographically protected encapsulation of

content, rights rules, and usage controls." (page 10, paragraphs [0139]-[0140]). However, nowhere in Shear et al. is there any disclosure that the "software container" is encrypted or verified by a hidden information stored in a hidden channel and changing the hidden information when said usage right information has changed.

With regard to the section of Shear et al. on pages 15-16, paragraphs [0216]-[0222], Applicants have studied this section which discloses that the disk may include an encrypted key block 208, that the key for decrypting the key block may be hidden on the disk or, alternatively, provided by the disk drive. Further, this section discloses that the disk may have secure containers for containing the keys. However, there is no disclosure of the nature of these "secure containers".

The Examiner indicates that Applicants' arguments concerning Downs et al., i.e., that the subject invention concerns a passive record carrier storing the information on a surface which is open for inspection, is not supported by the claims, and that in addition, claim 8 states that a record carrier could be a hard disc, which would not store information on a surface which is open for inspection.

Applicants submit that a careful reading of the specification as filed would reveal that the term "record carrier" as used in the claims is limited to, for example, optical discs, and hard disks. While a hard disk is normally enclosed within a

protective casing, the data is indeed stored on a surface of the hard disk, and that the surface of the hard disk is easily inspected by merely opening the protective casing. This is as opposed to an integrated circuit as described in Downs et al. which would require reverse engineering to uncover data stored therein.

Further, Applicants submit that both Downs et al. and Ginter et al. find it necessary to store keys within the end-user device, separate from the record carrier.

The Smithies et al. patent discloses a document and signature data capture system and method, in which, before encryption, "the contents of the signature envelope 10, together wit ha key provided by the client application 2, are checksummed using the same technique as is used for checksumming the file. Without knowledge of the key used by the original client application 2 when it caused the signature envelope 10 to be built, it would therefore be impractical to modify the signature envelope 10 and regenerate a satisfactory checksum."

However, Applicants submit that Smitbies et al. does not supply that which is missing from Shear et al., Downs et al. and Ginter et al., i.e., a record carrier storing a digital work and usage right information, in which the usage right information is updated with every use of the digital work, and that a hidden information stored in a hidden channel of the record carrier and

used to encrypt or verify the usage right information, is changed when the usage right information is changed.

In view of the above, Applicants believe that the subject invention, as claimed, is not rendered obvious by the prior art, either individually or collectively, and as such, is patentable thereover.

Applicants believe that this application, containing claims 1-13, is now in condition for allowance and such action is respectfully requested.

Respectfully submitted,

by 
Edward W. Goodman, Reg. 28,613
Attorney
Tel.: 914-333-9611